

## RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

### La technologie et le droit

Poullet, Yves

*Published in:*  
Mélanges G. Horsmans

*Publication date:*  
2004

*Document Version*  
le PDF de l'éditeur

[Link to publication](#)

*Citation for pulished version (HARVARD):*  
Poullet, Y 2004, La technologie et le droit: du défi à l'alliance. Dans *Mélanges G. Horsmans*. Académia Bruylant, Bruxelles, p. 943-967.

#### General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

#### Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

# LA TECHNOLOGIE ET LE DROIT DU DÉFI À L'ALLIANCE

PAR

Y. POULLET

PROF. AT THE UNIV. OF NAMUR AND LIEGE

DEAN OF THE FACULTY OF LAW OF NAMUR

DIRECTOR OF THE CRID

YVES.POULLET@FUNDP.AC.BE

[HTTP://WWW.DROIT.FUNDP.AC.BE/CRID](http://WWW.DROIT.FUNDP.AC.BE/CRID)

1. La participation au «*Liber Amicorum*» d'un collègue implique une opération délicate : celle du choix du sujet. Ce sujet doit permettre non seulement à celui-ci qui l'écrit de s'exprimer à l'aise mais surtout à celui-là à qui il est offert d'y retrouver soit le souvenir ému de leurs discussions, soit la découverte d'un domaine que ce dernier eût aimé couvrir et d'apparaître ainsi comme une invitation amicale à de «nouvelles» discussions.

Cher Guy, en choisissant de t'entretenir des relations contradictoires et ambiguës entre droit et technologies de l'information et de la communication, c'est la seconde branche de l'alternative que j'ai retenue. La sélection du thème répondait à une double conviction à propos de ta personnalité : ton amour de la modernité et ton souci de porter sur les choses qui t'entourent un regard critique loin des aphorismes.

Or sur les relations entre droit et technique<sup>(1)</sup> pèsent de nombreux aphorismes. N'entend-on pas comme une vérité révélée que le droit est toujours en retard sur une technique qui lui dicte son mouvement ? Ne jure-t-on pas que la technologie d'Internet révolutionne le droit ? Mon ambition n'est pas de répondre de manière définitive à ces interrogations mais en deux temps d'émettre quel-

(1) Sur les relations entre Droit et Technique, la thèse remarquable de S. GUTWIRTH, *Waarheidsuanspraken in Recht en wetenschap*, Antwerpen, Maklu, VUB Press, Thèse, 1993 en particulier, p. 462 et s. sur la fonction médiatrice autonome du droit face aux développements technologiques.

ques hypothèses : les premières cherchent à cerner les rôles de la technologie face au droit : rôle de remise en cause comme il est banal de l'affirmer, mais également de soutien des intérêts promus par le droit, au risque, nous le montrerons, d'une déformation de ce dernier (Titre I). Les secondes analysent comment le droit envisage le donné technologique en le soumettant à certaines contraintes voire en exigeant de lui qu'il soit au service du droit (Titre II).

Quelques conseils au juriste concluront l'examen de ces hypothèses.

## TITRE LA TECHNOLOGIE FACE AU DROIT

2. L'aspect révolutionnaire que représentent les développements des technologies de l'information et de la communication pour le droit est affirmé. Reste à en mesurer l'ampleur. Sur ce point, nous nous contenterons de quelques pistes (I).

Le rôle de la technologie comme alliée du droit est moins souvent souligné. Un tel rôle est cependant évident à l'heure actuelle où chacun réclame la sécurité sur Internet et comprend que celle-ci ne peut être acquise par la seule vertu de la loi mais le sera mieux encore par la technologie elle-même : «The answer to the machine is in the machine» proclamait dès 1996, Charles Clark (2). Sans doute, la sécurité réclamée sera-t-elle différente suivant que son besoin est affirmé par les investisseurs sur le Net ou par les citoyens consommateurs ou concernés par leurs données circulant sur le Net. Sans doute, et cela est important pour notre propos, la sécurité obtenue par la technologie ne sera-t-elle pas de la même nature que celle projetée par nos législations et cela au risque de fausser les équilibres consacrés par le Droit. Tel sera l'objet du point II de notre premier titre.

### A. - La remise en cause du droit par la technologie

3. Que le développement technologique offre à ceux qui le souhaitent le moyen de saper l'ordre réglementaire apparaît évident. Cette remise en cause s'opère à trois niveaux : le premier est sans doute le plus évident : le contenu des règles est ébranlé par des pra-

tiques que facilitent les technologies les plus récentes dans la mesure où le respect de telles règles est rendu difficile. Ce sera le premier point de notre réflexion. La deuxième remise en cause porte non point sur le contenu mais sur l'auteur des règles. La normalisation des comportements qu'induisent les choix technologiques, n'est plus le fait d'autorités habilitées par nos constitutions ou lois pour ce faire, mais par d'obscurées et peu transparentes autorités privées dont la légitimité est peu évidente. Le troisième point s'inquiète des conséquences du caractère global de la technologie, dimension qui induit la perte des souverainetés nationales, qui traditionnellement s'appuyaient sur leur territoire pour rendre effective la protection des règles et valeurs choisies démocratiquement.

#### 1. Un contenu ébranlé!

4. M. Froomkin (3) intitulait un article publié récemment : «The Death of Privacy». Selon l'auteur, exemples à l'appui, il démontrait combien le déploiement rapide des technologies tant par les administrations que par les entreprises rendait obsolètes les règles en matière de vie privée. D'autres auteurs (4) évoquent les «Privacy Killing Technologies», permettant le traçage des utilisations du Net, leur profilage, «l'Ubiquitous surveillance» (5), l'espionnage des systèmes d'informations (6), etc.

Les justifications avancées pour le développement de telles technologies reposent sur des arguments tant de sécurité publique (7),

(3) A. M. FROOMKIN, «The Death of Privacy?», 52 *Stanford Law Review*, 2000, p. 1461 et s.

(4) Ainsi J.-M. DINANT, «Electronic Threats on personal data and electronic data protection on the Internet, in Law and Technology Convergence» (Sect.5), *E-Commerce Law and Practice*, Edip Network, J. WALDEN & J. HORNLE (Ed.), Woodhead Publishing, 2002. M. ROTHENBERG «Fair Information Practices and the Architecture of Privacy», 2001 *Stan Tech L. Rev.* 1, n° 62 et s. ) parle de «Privacy Invasive Technologies» (PITS).

(5) Ainsi, le I.P. v. 6, nouveau protocole qui permettra d'assurer l'adressage de tous les terminaux utilisant l'Internet (soit outre les adresses I.P. actuelles, la nouvelle génération de téléphonie ou de mobilophonie utilisant l'Internet, les annuaires électroniques, etc.) et ce, indépendamment de leur localisation. (Sur ce nouveau protocole développé par l'IETF, lire G. LAWTON, «Is I.P. v 6 finally gaining Ground?», in *Computer IEEE Computer Society*, August 2001, p. 11-15 et surtout l'opinion 2/2002 (WP 58) émise par le groupe européen dit de l'article 29 sur l'utilisation de système d'identification unique dans les équipements terminaux : l'exemple de l'Ipv.6, 30 mai 2002).

(6) Depuis les «cookies», les concepteurs de systèmes d'information ont amélioré les techniques dites de Spyware (à leur propos, J.-M. DINANT, art. cité.). Sur tous ces systèmes, le document de travail (WP 37) du groupe dit de l'article 29 «Privacy on the Internet - An integrated Approach to On-Line Data Protection», 21 nov. 2000.

(7) Ainsi, l'autorisation donnée aux autorités de police et judiciaire d'accéder aux données de trafic et de localisation (cf. par exemple aux Etats-Unis, le projet Carnivore ou à l'échelle mondiale, le système Echelon).

(2) Ch. CLARK, «The answer to the machine, is in the machine», in *The Future of Privacy*, B. HUGENHOLTZ (Ed.), Kluwer, 1996, p. 139-146.

de lutte contre la criminalité informatique (8), que de la volonté d'améliorer le service à la clientèle par une intervention de maintenance directe sur les systèmes où sont installés les logiciels ou par un «one to one marketing».

5. Le pillage des «œuvres» sur Internet représente un autre souci majeur. La digitalisation des œuvres qu'elles soient sonores, visuelles ou écrites, les capacités des réseaux et des terminaux jointes aux technologies de compression expliquent ce fait. Napster dans un premier temps, les logiciels «peer to peer» comme Kazaa, Gnutella, Glockster, etc. ont largement illustré cette réalité. Certains (9) ont même pu s'écrier, il y a quelques années, que le droit d'auteur était mort ou, pour être plus exact, restait lettre morte au moment où la publication des copies de l'œuvre en des lieux ignorés et aux quatre coins du monde rendait vaines les poursuites.

## 2. Des «auteurs» sans statut constitutionnel

6. Dans un article publié en 1993, J. Reidenberg (10) soulignait déjà le hiatus entre deux mondes : celui de la réglementation des opérations et celui de la normalisation technique. Le premier monde ressortait indiscutablement de la compétence des législateurs nationaux traditionnels, simplement l'ampleur des questions nécessitant de plus en plus des coopérations au sein des organisations internationales ou régionales. Le second monde émergeait à l'époque : la normalisation d'une infrastructure globale comme celle d'Internet exigeait des décisions qui ne pouvaient être prises qu'au sein des organes dits de régulation technique, aux compétences encore balbutiantes, organes que les pionniers d'Internet avaient mis au point (11).

(8) En particulier, la lutte contre le copiage illicite d'œuvres. Sur ce phénomène, les chiffres et études mentionnées par Jan KASTNER, «Law and Technology Convergence: copyright», in *E-commerce Law and Practice in Europe*, ECLIP Network, I. WALDEN et J. HORNLE, Woodhead Publishing Ltd, Cambridge, 2001.

(9) Cf. notamment, T. VINJE, «A brave new world of technical Protection: will there still be a room for copyright?», *EIPR*, 1996, n° 8, p. 430 et s.

(10) J. REIDENBERG, «Rules of the Road on Global Electronic Highways: Merging the Trade and Technical Paradigms», 6 *Harvard J. Law & Tech.*, 1993, 287. Du même auteur, on notera les articles parus depuis, «Governing Networks and Rule-Making in Cyberspace», 45 *Emory Law Journal*, 1996, 912-930; «Lex Informatica: The Formulation of Information Policy Rules through Technology», 76 *Texas Law Rev.*, 1998, 553-593.

(11) Sur ces différents organes de normalisation technique en matière de technologies de l'information et de la communication, lire P. TRUDEL (Ed.), *Droit du cyberspace*, Montréal, Thémis, 1997; J. BERLEUR-Y. POULLET, «Quelles régulations pour l'Internet», in *Gouvernance de la société de l'information*, Cahier du CRID, n° 22, Bruxelles, Bruylant, p. 133 et s.

Ces organes, comme l'IETF (12), le W3C (13), l'IANA devenue l'ICANN (14), ont, en même temps qu'Internet tissait sa toile, acquis, sans renier leur statut d'origine, leurs lettres de noblesse parfois avec la complicité de gouvernements (15) ou d'organisations internationales (16). Qui ne comprend qu'au-delà d'une normalisation technique, comme l'attribution de noms de domaines (17), l'adressage sur Internet, les design de l'infrastructure, la définition de protocoles techniques de filtrage des contenus, etc., il s'agit de décisions dont le contenu en un autre temps eût été pris par des auteurs, objet d'une légitimité constitutionnelle (18)? Une telle assertion est à la base même de l'ouvrage qui, sans aucun doute, a le plus marqué la littérature juridique voire l'opinion publique sur les relations entre droit et technologie : «Code and other Laws of Cyberspace» de Lawrence Lessig (19). Selon L. Lessig, l'architecture technique, les caractéristiques du réseau (les protocoles, les standards de communication retenus,...) créent un environnement auto-

(12) Sur l'Internet Engineering Task Force (I.E.T.F.), lire M.A. FROOMKIN, «Habermas @ discourse.net: Toward a critical theory of cyberspaces», 116 *Harv. Law Rev.*, p. 800 et s. (2003); S. BRADNER, «IETF Working Group Guidelines and Procedures», disponible sur le site <http://www.ietf.org/rfc>

(13) A propos du W3C qui contrôle le développement du HTML et des autres standards du Web, lire S.L. GARFINKEL, «The Web's unelected Governments», *MIT Technology Review*, 38.46 (Nov/Déc 98) disponible sur le site <http://www.technologyreview.com/articles/garfinkel.1198.asp> Pour le fonctionnement du W3C et ses liens avec l'IETF, voir le site du W3C <http://www.w3c.org/consortium>

(14) Sur l'histoire de l'ICANN, voir J. WEINBERG, «ICANN and the problem of legitimacy», 50 *Duke Law Journal*, 187 (2000).

(15) A cet égard, à propos du soutien du Department of Commerce américain à la création de l'ICANN et de la volonté du gouvernement américain de garder par l'ICANN le contrôle de la gouvernance de l'Internet, lire les articles de A.M. FROOMKIN, «Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution», 50 *Duke L.J.*, 17 (2000); «Form and Substance in Cyberspace», *Northwestern School of Law of Lewis & Clark College*, 93 et s. (2002).

(16) Ainsi les liens entre l'OMPI et l'ICANN. Par contre, à noter, le combat en 1992 entre l'IETF et l'ISO (International Standard Organisation); sur le choix entre le protocole TCP/IP et le modèle en couches OSI. On sait que c'est finalement le choix de l'organisation privée qui l'emporta.

(17) A ce sujet, le remarquable article de J. REIDENBERG, «Lex Informatica: The formulation of Information Policy Rules through Technology», 76 *Texas L. Review*, 1998, p. 553-584 et l'ouvrage de base de L. LESSIG, *Code and Other Laws of Cyberspace*, New-York, Basic Book, 1999.

(18) A propos de la légitimité contestable des organes de normalisation technique, lire A.M. FROOMKIN, «Habermas@discourse.net: Toward a critical theory of Cyberspaces», 116, *Harv. Law Review*, p. 731 et s. (2003). Sur cette émergence des «pouvoirs» privés et leur rôle réglementaire, lire F. OST et M. van de KERCKHOVE, «De la pyramide au réseau! Vers un nouveau mode de production du droit», *Rev. Interdiscipl. d'études juridiques*, 2000, 44, p. 66 et s.

(19) L. LESSIG, *Code and other Laws of Cyberspace*, New York, Basic Books, 1999 (disponible sur le site : <http://www.cyberlaw.stanford.edu/lessig/content/index.html>). Selon Lessig, la régulation d'Internet résulte de l'interaction de quatre modes de régulation : la loi, les normes sociales, le marché et surtout l'architecture technique.

risant certains comportements et en interdisant d'autres et jouent donc un rôle essentiel dans la régulation du cyberspace. Par ailleurs, il est remarquable de constater que les législateurs et juges devront tenir compte de ce donné décidé ailleurs des enceintes traditionnelles du droit (20).

### 3. La remise en cause de l'Etat souverain

7. L'Etat national exerçait dans le cadre de son territoire, sa souveraineté (21). La technologie remet en cause cette «souveraineté» à plus d'un titre :

- la dématérialisation facile des investissements principalement immatériels que représente l'innovation technologique. Ce fait pousse nos Etats soit à harmoniser leurs législations (22), soit à se lancer dans une sorte de dumping réglementaire (23) apte à attirer de tels investissements.
- L'abolition des frontières : l'architecture même de l'infrastructure, son maillage et l'abolition de la distance comme facteur de coût de la transmission, conduisent à la multiplication des flux trans-frontières conscients ou inconscients. On notera que la majorité des root-servers d'Internet sont localisés aux Etats-Unis (24) et

(20) Sur cette interaction entre la régulation technique et la régulation traditionnelle, lire J. REIDENBERG, «Privacy Protection and the Interdependence of Law, Technology and Self-regulation», in *Variations sur le droit de la société de l'information*, Cahier du CRID, n° 20, p. 130 et s.; Yves POULLET, «How to regulate Internet: New Paradigms for Internet Governance», publié dans le même ouvrage, p. 79 et s.

(21) Sur les liens intimes entre «territorialité et Etat» et leur remise en cause par l'émergence de l'immatériel, lire H. Ruiz FARRI, «Immatériel, territorialité et Etat», *Arch. phil. droit*, T. 43, 1999, p. 187-212; «Le développement des communications immatérielles et la porosité de l'Etat à leurs mouvements posent la question de la maîtrise de l'Etat d'un espace normatif national normalement calqué sur le territoire et exprimé dans le principe de territorialité». Cf. également, F. CONSTANTIN, «L'informel internationalisé ou la subversion de la territorialité», in B. BADIE et M.-C. SMOUTS (Eds), *L'international sans territoire, Cultures et conflits*, n° 21/22, 1996, p. 311-345.

(22) Dans un article récent («Vers la Confiance: Vues de Bruxelles - Quelques considérations sur la spécificité de l'approche réglementaire européenne du cyberspace», *Lamy Droit de l'informatique et des réseaux*, 2001, n° 141 et 142) l'auteur décrit amplement ce phénomène au niveau européen et les modes d'harmonisation retenus.

(23) Sur ce phénomène, R. QUECK, Y. POULLET, «Internet face au droit: Conclusions», in *Internet face au droit*, Cahier du CRID n° 12, 1997, p. 231-247. En matière de propriété intellectuelle, ce sera au contraire, le pays qui offrira le maximum de protection qui attirera l'investissement, D.L. BURK, «Virtual Exit in the Global Information Economy», 73 *Chicago Kent L. Rev.*, 1999, n° 4, p. 953 et 954; «We may therefore expect that a jurisdiction's intellectual property comparative advantage may assume considerable importance in determining the physical location of information producers». L'auteur démontre (p. 970 et s.), en reprenant le «dilemme du prisonnier», les raisons qui peuvent pousser les régulateurs à coopérer ou à l'inverse à préférer la concurrence.

(24) On compte 10 routeurs sur 13 localisés aux Etats-Unis.

que la transmission des messages via satellites ou autres médias de transmission peut faire l'objet d'interception par des puissances étrangères (25).

Sans doute, les règles de droit international privé permettent-elles encore à nos tribunaux d'affirmer la prééminence de la loi nationale souveraine (26) mais leur décision se heurtera souvent à l'impossibilité d'en assurer l'application dans le cadre d'un réseau sans frontières (27).

### B. La technologie au secours du droit

8. Par un second mouvement quasi opposé au premier, la technologie se met au secours du droit. Dans un premier temps, notre propos est de décrire ce mouvement dans deux domaines : celui de la privacy et de la propriété intellectuelle, quelques développements technologiques dont l'objectif est clairement d'assurer la protection d'intérêts par ailleurs protégés par le droit. Si l'expression de «Privacy Enhancing Technologies» (PETS) (28) a ainsi été promue pour désigner des technologies protectrices de notre vie privée, on peut désormais de manière parallèle parler de «Intellectual Property Enhancing Technologies» (IPETS) (29) voire de «Consumer Protection Enhancing Technologies»

(25) C'est le cas du réseau d'écoutes satellitaires Echelon. Sur Echelon, lire J.M. DINANT et Y. POULLET, «Le réseau Echelon existe-t-il?», disponible sur le site du CRID à <http://www.crid.ac.be> et surtout D. YERNAULT, «De la fiction à la réalité : le programme d'espionnage électronique global «Echelon» et la responsabilité internationale des Etats au regard de la Convention européenne des droits de l'Homme», *Rev. Belge de droit int.*, 2000, p.136 et s.

(26) A cet égard, la thèse récemment défendue par B. de GROOTE, *Onrechtmatige daad en Internet. Een rechtvergelijkende analyse van art. 5, sub. 3 EEX Verordening en de Amerikaanse bevoegdheidsregeling aan de hand van het internet*, Thèse, RUG, 24 janvier 2003, en voie de publication.

(27) L'affaire Yahoo illustre à suffisance cette vérité. Dans ce cas les ordonnances du tribunal parisien des 22 mai et 20 novembre 2000 (disponible sur le site <http://www.juriscom.net> avec tout un dossier consacré à l'affaire) obligeaient Yahoo, société américaine, à filtrer à l'attention des internautes français certains sites révisionnistes illégaux au regard du droit français. Ces ordonnances ont été considérées comme contraires à la liberté d'expression par le tribunal de San Diego (*Yahoo Inc. v. LICRA*, July 7, US. District Court California, San Jose Div.) car contraire au principe de la liberté d'expression. Sur ce cas, lire J. REIDENBERG, «Companies will have to comply with the laws where they target business» disponible à l'adresse : <http://www.juriscope.net/en/unidoc/yahoo/reidenberg.htm>

(28) Sur cette terminologie et une typologie des PETS, lire parmi d'autres, H. BURKERT, «Privacy Enhancing Technologies: Typology, Critique, Vision» in AGRE & RUTENBERG (Eds), *Technology and Privacy: new Landscape*, New York, 1992.

(29) Sur ces multiples formes de technologies protectrices du copyright, lire Jan KAESTNER, «Law and Technology Convergence: Copyrights», in *E-commerce: Law and Practice*, ECLIP Network, I WALDEN and J. HORSTLE (Eds), Woodhead Publishing Limited, London.

(CPETS) (30) bref regrouper l'ensemble de ces technologies sous le vocable générique de «Rights Enhancing Technologies» (RETS).

Dans un second temps, il s'agira de montrer à travers les mêmes exemples, combien nonobstant l'identité des intérêts protégés, les technologies modifient sensiblement les paradigmes à la base des législations consacrant ces mêmes intérêts.

### 1. A propos des «Rights Enhancing Technologies»

9. Avant d'aborder les deux domaines retenus : les PETS et IPETS, soulignons ce qui en a constitué sans doute historiquement le premier exemple et relevons la portée de celui-ci. On se souviendra que le législateur américain avait estimé nécessaire une solution législative spécifique pour lutter contre les messages dommageables en particulier envers les mineurs et avait adopté une loi connue sous l'appellation de «Decency Act». La Cour constitutionnelle jugea le texte législatif contraire au premier amendement (31). Parmi les nombreux arguments, l'un pesa sans doute de manière importante, la restriction légale à la liberté d'expression n'est point nécessaire là où des mesures technologiques moins restrictives pour la liberté d'expression permettent d'assurer la protection voulue (32). Tels étaient l'enjeu et l'objectif du développement par le W3C des «Platforms for Internet Content Selection» (les PICS) (33).

Il s'agirait par un système logiciel lié à une labellisation des sites web de permettre aux parents de définir a priori les sites acceptables et ce à divers points de vue : «vocabulaire, sexe, nudité,

(30) Ce néologisme désigne toute une série de technologies permettant une meilleure information du consommateur (p.ex. système de flickering permettant au consommateur d'avoir l'attention attirée vers certaines clauses du contrat, système de pop-up apparaissant automatiquement pour donner quelques explications supplémentaires), une meilleure négociation du contrat conclu électroniquement (p.ex. système récapitulatif des transactions opérées, système de détection automatique d'erreur, etc.), une meilleure conservation de la transaction (système d'archivage avec accès direct à l'opération conclue) voire des facilités en cas de problèmes liés à l'exécution du contrat (hot line, système de négociation on line en cas de plainte, possibilité d'accès à un système électronique de médiation, etc.).

(31) Sur la genèse du Decency Act et sa critique par la Cour constitutionnelle, lire D. CUSTOS, «Liberté d'expression des adultes et protection des mineurs sur le réseau Internet selon la Cour suprême des États-Unis», *Reno v. ACLU*, 26 juin 1997, *Rev. Dr. Public*, 1998, p. 45 et s.; C. LAMOULINE et Y. POULLET, *Des autoroutes de l'information à la «démocratie électronique. De l'impact des technologies de l'information et de la communication sur nos libertés»*, Rapport pour le Conseil de l'Europe, Bruxelles, Nemesis, Bruylant, 1997, en particulier les p. 60 et s.

(32) Sur ce débat, lire L. LESSIG, *Code and other Laws in Cyberspace*, Basic Books, New York, 1999, p. 177 et s.

(33) Le lecteur trouvera une bonne description des PICS en R.P. WAGNER, «Filters and the First Amendment», 83 *Minn. L. Rev.*, (1998), p. 755 et s.

violence». Notre propos n'est pas ici de rappeler quelques critiques adressées par ailleurs mais de souligner l'intérêt d'un système technique dont l'effectivité est bien plus grande que celui reposant sur les secours judiciaires à l'entame coûteuse, à l'issue aléatoire et à «l'enforcement» douteux dans un contexte international. Que la réponse technologique ait été en la matière préférée à la réponse législative en tout cas telle que proposée ne surprendra personne (34).

10. Les mêmes principes animent la «Platform for Privacy Preferences» (35) mise au point dans le cadre des travaux du W3C et considérée comme la forme la plus achevée des PETS. Il s'agit de mettre à disposition de celui qui le souhaite un outil permettant à chacun de définir ses préférences en matière de vie privée, d'exclure a priori toute visite de site Internet ne respectant pas de telles préférences quitte à autoriser a posteriori le dialogue avec de tels sites pour obtenir tel ou tel avantage en échange de données ou de l'autorisation d'utilisation de telle ou telle donnée (36).

11. Dans le domaine des IPETS (37), on relève de nombreuses solutions dont certaines visent à restreindre l'accès; d'autres à contrôler voire restreindre a priori l'utilisation ou certaines utilisations, d'autres enfin, à constater a posteriori l'utilisation illicite. Dans tous les cas, elles garantissent que les intérêts des détenteurs de droits ou plus largement des personnes ayant mis sur le marché l'information protégée sont efficacement protégés. Elles constituent

(34) Sur l'évolution des approches depuis l'approche législative du Decency Act, l'approche autoréglementaire pure des PICS et de la fondation Bertelsmann jusqu'à l'approche dite de co-régulation présente en Europe sur le modèle australien, lire M. d'UDEKEM-GEYERS et Y. POULLET, «Internet Content regulation: Concerns from a European User Empowerment Perspective about Internet Content Regulations», *CL&SR*, 2001, p. 371 et s.

(35) «I welcome this important new tool for Privacy Protection. It will empower individuals to maintain control over their personal information while using the World Wide Web». Cette déclaration figure en exergue de la première publication du W3C à propos du P3P alors non encore existant (W3C first Public Working Draft of P3P 1.0 Testimonials (19 mai 1998), publié sur le site du W3C à l'adresse : <http://www.w3.org/Press/1998/P3P.html>).

(36) Sur le P3P et son fonctionnement, lire L.F. CRANOR, *Agents of Choice: Tools that facilitate Notice and Choice about Web Site Data Practices*, disponible sur le site : <http://www.research.att.com/~lorrie/pubs/hk.pdf>.

(37) A cet égard, les travaux d'IMPRIMATUR, et notamment la publication de A. DE KROON, «Protection of Copyright Management Information», Amsterdam, Déc. 98 disponible sur le site d'Imprimatur : [http://www.imprimatur.ales.co.uk/IMP\\_FTP/emil.pdf](http://www.imprimatur.ales.co.uk/IMP_FTP/emil.pdf) qui reprend une liste très complète des technologies de protection; cf. également A. STROWEL et S. DUSOLLIER, *La protection légale des systèmes techniques. Atelier sur les questions relatives à la mise en œuvre des traités de l'OMPI de 1996*, Genève, 6-7 déc. 1999.

en ce sens une réponse aux craintes d'un cyberspace de pirates, soulignés ci-avant.

Pour contribuer encore à l'efficacité de telles mesures techniques, le droit lui-même a cru bon d'ajouter une couche supplémentaire de protection : la mise au point ou l'utilisation de système de contournement des mesures technologiques est en soi, affirme l'OMPI passible de sanctions dont l'ampleur est laissée aux différents États (38). La technologie vient au secours du droit qui lui-même, échange de bons procédés, vient au secours de cette technologie. Mais n'anticipons pas sur le rôle du droit face à la technologie et examinons plutôt à travers les exemples du P3P et des DRMS, comment une technologie certes aux effets protecteurs remet en cause l'esprit, les paradigmes inscrits au cœur des législations de protection de la vie privée, d'une part, de propriété intellectuelle, d'autre part.

## 2. Les changements «paradigmatiques» opérés par les «Rights Enhancing Technologies»

### - l'exemple du P3P (39)

12. Le P.3.P., comme déjà les PICS, est une technologie construite autour du mythe de «l'User Empowerment» (40). C'est, grâce à la vertu du paramétrage de son navigateur, l'internaute qui décide des données qu'il consentira à transférer, des utilisations

(38) Il s'agit de l'article 11 du Traité sur le droit d'auteur adopté par la conférence diplomatique de l'OMPI en 1996 : «les parties doivent prévoir une protection juridique et appropriée et des sanctions juridiques efficaces contre la neutralisation des mesures techniques efficaces, qui sont mises en œuvre par l'auteur dans le cadre de l'exercice de leurs droits...». Sur cette question, lire S. DUSOLLIER et A. STROWEL, «La protection légale des systèmes techniques : analyse de la directive 2001/29 sur le droit d'auteur dans une perspective comparatiste», *Propriétés intellectuelles*, 2001, p. 10-27.

(39) A propos du P3P, lire J. REAGLE-L. FAITH, «The Platform for Privacy Preferences», *Comm. Of the ACM*, Feb. 99, vol. 42, n° 2, 48-55, la description sur le site du W3C, <http://www.w3.org/TR/WD-P3P-preferences> et la critique du Groupe européen dit de l'article 29 créée par la directive 95/47 relative à la protection des données : Opinion 1/98 : Platform for Privacy Preferences (P3P) and the Open Profiling Standards (OPS) : <http://europa.eu.int/comm/dg15/en/media/dataprot/wpdoes/wp11fr.pdf>. A noter également les réflexions de P.M. SCHWARTZ, «Beyond Lessig's Code for Internet Privacy : Cyberspace Filters, Privacy Control, and Fair information practices», *Wiscounsin Law review*, 2000, p. 749 et s.

(40) «Central to this concept of user empowerment is the recognition that, on the internet, individuals and parents are best situated to make decisions about what information flows into the home» (Center for Democracy and technology, An analysis of the Bertelsman Foundation Memorandum, disponible sur le site du centre : <http://www.cdt.org>). Sur cette notion déjà utilisée à propos des PICS et des techniques de contrôle individuel des contenus illicites ou dommageables sur Internet, lire M.D'UDEKEM-GEVERS et Y. POULLET, article cité.

tions qui pourront en être faites, de l'utilisation ou non d'un pseudonyme etc. Le cas échéant, il renoncera, mais n'est-ce point là son droit, à la protection qu'il s'était lui-même attribuée (41). Une telle approche repose en définitive sur une conception de la vie privée vue comme une «propriété» de ses données personnelles. Cette propriété fonde autant l'exclusion d'autrui de toute utilisation de mes données que la «vente» ou du moins la cession d'utilisation de données désormais vues comme des «commodités», des valeurs marchandes. Une telle approche, on le pressent, est à distance de celle proposée par nos législations «Privacy». Si ces législations reconnaissent le consentement comme un des fondements possibles de légitimité du traitement de données à caractère personnel, elles ne le reconnaissent jamais comme suffisant (42) dans la mesure où tout traitement doit être évalué non du seul point de vue individuel de la personne concernée mais de manière plus collective dans le cadre des pouvoirs des collecteurs d'informations, pouvoirs que l'utilisation de l'information relative à autrui contribue à renforcer (43).

Ce contrôle justifie l'intervention de l'Etat et en particulier tant d'une législation consacrant la nécessité de maintenir un équilibre informationnel entre la personne concernée et le responsable de traitements que l'intervention d'une autorité indépendante de contrôle

(41) Cf. la description donnée par Lessig du P3P : «The user sets her preferences once-specified how she would negotiate privacy and what she is willing to give up, and from that moment on, when she enters a site and her machine negotiate. Only if the machine can agree will the site be able to obtain her personal data.» (L. LESSIG, «Code and other laws of cyberspace», *op. cit.*, p. 160 et 161). Pour plus de renseignement sur cette plate-forme, voir le site : <http://w3c.org/P3P.htm>

(42) A ce propos, A. PIERUCCI, «Le rôle du consentement de la personne concernée dans le marketing électronique», *Ubiquité*, 2001, n° 9 ; T. LÉONARD, «E-commerce et protection des données à caractère personnel, Quelques considérations sur la licéité des pratiques nouvelles de marketing sur Internet», in *Internet & Recht*, Antwerpen, Maklu, 2001, p. 418 et s.

(43) Comp. «Consent-based approaches to information rights are weak, more fundamentally, because they do not recognize parameter-setting acts of consent or refusal by society as a whole. Problems of market power and cognitive disability could be offset to a degree by coercitive legislation. Consent is definitively atomistic and the political process is definitionally coercitive» (J.E. COHEN, «Information Rights and intellectual Freedom», in *X. Ethics and the Internet*, Anvers, Intersentia, 2001, p. 11 et s.). Dans le même sens sur cette critique de la «propretization» de la vie privée par l'effet de technique comme le P3P, l'article remarquable de P.M. SCHWARTZ, «Beyond Lessig's Code for Internet Privacy», *Wisconsin Law Review*, 2000, p. 743 et s. (en particulier, p. 787). De manière plus générale sur la comparaison de l'approche américaine fondée sur la propriété des données à caractère personnel par opposition à l'approche européenne fondée sur un contrôle sociétal, lire Y. POULLET, «Pour une justification des articles 25 et 26 en matière de flux trans-frontières», Rapport présenté à la réunion européenne : The Future of the European Data Protection Directive, Nov. 2002. *Mélanges offerts à Bart de Schutter*, VUB Press, 2003, à paraître.

pouvant intervenir à ce propos (44). Il s'agit de régler des conflits non de propriété comme le laisseraient à penser les mesures technologiques mais des conflits de libertés susceptibles d'être remises en cause à partir du moment, soit où faute de moyens intellectuels ou financiers, la personne concernée n'est pas libre de son choix d'assurer ou non la protection de ces données, soit où la transparence de ce dernier est telle que ces choix en seront influencés voire dictés.

– l'exemple des D.R.M.S.

13. Séverine Dusollier (45) écrit : « Dans l'environnement analogique, l'accès à l'œuvre par le public et sa consultation ne nécessitent aucune autorisation de l'auteur. Lire un livre, voir un film, assister à un spectacle, regarder des œuvres plastiques n'implique généralement dans le chef de l'utilisateur, aucun acte soumis au droit d'auteur, qu'il s'agisse d'un droit de reproduction ou de communication au public ».

Certains dispositifs techniques de gestion d'accès aux œuvres permettent de contrôler non seulement l'accès initial à l'œuvre, mais de vérifier à chaque nouvel accès les conditions d'utilisation, de fixer le prix en fonction du type d'utilisation demandé ou d'exiger un paiement renouvelé à chaque utilisation. Ces systèmes s'appuient sur l'envoi de mots de passe ou l'utilisation de techniques de cryptographie (46). Ayant ainsi décrit ces technologies, l'auteur (47) conclut : « En matière de cryptographie et d'accès sécurisé, la technique n'épouse plus parfaitement les prérogatives de l'auteur. Il ne s'agit plus seulement de renforcer l'effectivité des droits exclusifs,

(44) L'article 8 de la Charte européenne des Droits de l'Homme consacre le droit à la protection des données de manière distincte du droit à la vie privée de manière à affirmer ce contrôle nécessaire des finalités d'un traitement et l'existence d'une autorité indépendante de contrôle, sur cet article 8, lire Y. POULLET, « Le droit et le devoir de l'Union européenne et des Etats membres de veiller au respect de la protection des données dans le commerce mondial », in *Le droit et le devoir de l'Union européenne et des Etats membres de veiller à la protection des données personnelles*, à paraître dans un ouvrage collectif publié pour le XXV<sup>ème</sup> anniversaire de la Constitution espagnole, Madrid, Dykinson, 2003, n° 11 et s.

(45) S. DUSOLLIER, « Incidences et réalités d'un droit de contrôler l'accès aux œuvres en droit européen », in *Le droit d'auteur : un contrôle de l'accès aux œuvres*, Cahier du CRID n° 18, Bruxelles, Bruylant, 2000, p. 26 et s.

(46) Ces différentes techniques sont décrites de manière très détaillée par J. KAESTNER, *op. cit.* Cf. également D. GERVAIS, « Electronic Copyright Management Systems in a Network environment », disponible à <http://www.Copyright.com/sruff/ERMSnetwork.htm> et du même auteur, « The Law and Practice of Digital Encryptions », Mai 1998 disponible sur le site [http://www.imprimatur.ales.co.uk/IMP\\_FTP/encryption.pdf](http://www.imprimatur.ales.co.uk/IMP_FTP/encryption.pdf)

(47) S. DUSOLLIER, *op. cit.*, p. 40 et 41 ; T. VINJE, « A brave new world of technical protection systems : will there still be room for copyright », *EIPR*, 1996, n° 8, 431.

droits de reproduction, de communication ou droit moral, par exemple, par le fait de la technique mais bien d'exercer de manière automatisée la gestion d'un service de distribution de contenus digitaux, qu'ils soient protégés par le droit d'auteur ou non (48). Par ailleurs, de tels systèmes de protection technologique des œuvres mettent à mal la possibilité de se prévaloir d'une série d'exceptions au droit d'exploitation de l'auteur que le législateur avait consenties précisément pour favoriser la création intellectuelle.

Progressivement, grâce à ces mesures technologiques, « It has become conventional to equate ownership of intellectual property with perfect control ... In the context of intellectual property, however, the economic justification for ownership – as – perfect – control is contested... »

« A system of intellectual property rules and rights designed to promote intellectual freedom also must consider the conditions of public access to and use of intellectual goods... Defining ownership as perfect control forecloses evaluation of these shifts in the distribution of costs and benefits flowing from the intellectual property regime and the resulting effects on intellectual freedom » (49)

## RE II. LE DROIT FACE À LA TECHNOLOGIE

14. La position du droit face à la technologie est double. Il s'agit d'abord d'accueillir le développement que représente l'innovation technologique veillant, selon le principe de neutralité technologique, d'une part, à ne point le discriminer mais, d'autre part, à ne point le favoriser. Ces deux premiers mouvements feront l'objet d'un premier point. Le droit peut par ailleurs, se montrer exigeant et tenant compte des possibilités que recèle la technologie, d'exiger que des choix soient imposés à son développement tantôt pour garantir la

(48) S. DUSOLLIER, *op. cit.*, p. 41 ; J. COHEN, « Information Rights and Intellectual Freedom », in *Ethics and the Internet*, Ant. VEDDER (Ed), Antwerpen, Intersentia, 2001, p. 20.

(49) J. COHEN, *op. cit.*, p. 27. Même réflexion chez A. DIAS-PEREIRA, « Copyright issues of techno-Digital Property », in *Intellectual Property in the digital Age: Challenges for Asia*, C. HEATH & A.K. SANDERS éd., Kluwer, 2001, p. 66 : « The concept of property has a major role in Digitalia and it seems to make sense. However some argued that the new wine could not fit in the old bottles. The new wine would be digital Information property and technologies and the old bottles would be traditional legal concept, in particular copyright and other forms of intellectual property ». Cf. à cet égard, l'article de P. Samuelson (« The Copyright Grabbed, Wired », 1996, cité par Pereira, art. cité, p. 67), qui définit l'« agenda maximaliste » des sociétés d'ayant droit, visant à transformer progressivement le droit de propriété intellectuelle en un droit de propriété pur et simple.



conformité avec le droit des opérations que la technologie permet, tantôt pour améliorer encore la protection des utilisateurs de celle-ci. Ces deux dernières attitudes du droit feront l'objet du second point.

#### A. – Le droit accueille de façon neutre la technologie

15. L'introduction révélait à cet égard deux significations du principe de la neutralité technologique : par la première, il s'agissait d'éviter que le droit ne constitue une barrière au développement de la technologie (principe de non-discrimination). Cette attitude caractérise particulièrement des législations récentes en matière de preuve et de signature. Ces mêmes législations nous permettront d'illustrer la seconde tendance : il ne peut être question par ailleurs de soustraire les développements technologiques des exigences présentes dans les législations traditionnelles. La théorie des «équivalents fonctionnels» développée à propos de la signature électronique et singulièrement élargie depuis, en témoigne. Dans le domaine de la lutte contre la criminalité informatique, ce même principe de neutralité technologique a conduit à affirmer le principe que ce qui était puni off line devait également l'être ni plus ni moins on-line.

#### 1. Du principe de la «non-discrimination» à celui de l'équivalence fonctionnelle (50) : le droit de la preuve et de la signature électronique

16. Le principe de «non-discrimination» est clairement consacré par deux directives récentes, l'une relative à la signature électronique, l'autre relative à certains aspects du commerce électronique.

On cite ainsi l'article 5.2 de la directive 1999/93/CE du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques (51) qui stipule : «les Etats membres veillent à ce que l'efficacité juridique et la recevabilité comme preuve en justice ne soient pas refusées à une

signature électronique au seul motif que la signature se présente sous forme électronique ou qu'elle ne repose pas sur un certificat qualifié délivré par un prestataire accrédité de service de certification ou encore qu'elle n'est pas créée par un dispositif sécurisé de création de signature». L'article 9.1 de la directive 2000/31/CE du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information (52) fait écho en des termes quasi semblables au même principe : «les Etats membres veillent à ce que leur système rende possible la conclusion des contrats par voie électronique. Les Etats membres veillent notamment à ce que le régime juridique applicable au processus contractuel ne fasse pas obstacle à l'utilisation des contrats électroniques ni ne conduise à priver d'effet et de validité juridique de tels contrats pour le motif qu'ils sont passés par voie électronique.»

17. Si la règle de non-discrimination se lit comme une approche négative du principe de neutralité technologique : «on ne peut exclure le donné technologique au seul motif que...», la théorie de l'équivalent fonctionnel en constitue l'approche positive : «le donné technologique a une valeur juridique égale à celle conférée au donné traditionnel à condition qu'il démontre sa capacité de réaliser les mêmes fonctionnalités que le donné traditionnel. Cette thèse exprimée pour la première fois en 1995 par un ouvrage du CRID à propos de la preuve électronique (53) a depuis été largement développée par les instances internationales (54) et européennes en matière de signature et d'écrit (55) et prolongée en Belgique de manière originale à propos du formalisme contractuel. Ainsi, l'article 16 de la loi du 17 mars 2003 (56) affirme que «toute exigence légale ou réglementaire de

(52) J.O. 17 juillet 2000, L 178/1. Sur cette disposition, lire notamment P. LECOQ et C. BIQUET-MATHIEU, «Le commerce électronique : conclusion et preuve du contrat», Rapport de droit belge in *Actes du Congrès de Brisbane*, Juillet 2002, Bruylant.

(53) M. ANTOINE, J.F. BRAKELAND et M. ELOY, *Le droit de la preuve face aux nouvelles technologies de l'information*, Cahier du CRID n° 7, 1995, Story-Scientia, Bruxelles.

(54) Cf. à ce propos, le Guide pour l'incorporation en droit interne de la loi type de la CNU-DCI sur le commerce électronique, 1996, en particulier le n°16 qui détaille de manière précise les fonctionnalités de l'écrit.

(55) Notamment, parmi de nombreux auteurs, M. DEMOULIN et E. MONTERO, «La conclusion des contrats par voie électronique», in *Le processus de formation du contrat. Contributions comparatives et interdisciplinaires à l'harmonisation du droit européen*, M. FONTAINE (Ed.), Bruxelles-Paris, Bruylant-LGDJ., 2002, Vol. 57, p. 550 et s. Les auteurs donnent un autre exemple de définition fonctionnelle, celle du «support durable», visant certains supports traditionnels comme certains supports numériques, notion utilisée par la directive 97/7 dite «contrats à distance» et définie enfin par la directive du 23 septembre 2002 sur la commercialisation à distance des services financiers.

(56) Loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information, *M.B.*, 17 mars 2003, p. 12693.

(50) Sur cette notion d'équivalent fonctionnel, lire en doctrine internationale, E. CAPRIOLI et R. SORREUIL, «Le commerce international électronique : vers l'émergence de règles juridiques transnationales», *JDI*, 2, 1997, en particulier, p. 380-382; en droit belge, D. GOBERT et E. MONTERO, «La signature dans les contrats et les paiements électroniques : l'approche fonctionnelle», *DA/OR*, n° 53, 2000, p. 17-39.

(51) J.O. 19 janvier 2000, L13/12. Sur cette disposition, lire parmi de nombreux auteurs, M. ANTOINE et D. GOBERT, «La directive européenne sur la signature électronique. Vers la sécurisation des transactions sur Internet !», *JTDE*, 2000, p. 73 et s.; D. MOUGENOT, «Droit des obligations - La preuve», *Rép. not.*, tiré à part, Bruxelles, Larcier, 3<sup>ème</sup> éd., 2002, n° 121 et s. (p. 168 et s.).

forme relative au processus contractuel est réputée satisfaite à l'égard d'un contrat par voie électronique lorsque les qualités fonctionnelles de cette exigence sont préservées». Montero (57) justifiait cette disposition comme suit : «En présence d'un tel obstacle (à savoir celui né de l'impossibilité de réaliser les exigences formelles imposées par les dispositions réglementaires consacrant le formalisme contractuel), l'article 16 §1<sup>er</sup> nous invite à adopter une approche dite «fonctionnelle». Il s'agit de rechercher quelles sont les qualités fonctionnelles de la formalité considérée, puis de vérifier si le procédé utilisé pour conclure le contrat par voie électronique permet de préserver ces qualités. Dans l'affirmative, l'exigence de forme est réputée rencontrée par le procédé en question et le contrat conclu par voie électronique ne peut être remis en cause à cet égard.»

Ainsi le droit reconnaît comme son devoir d'accueillir les développements technologiques qui se substituent aux processus traditionnels de conclusion de mise en œuvre ou de conservation des contrats lorsque ces développements garantissent le respect des exigences fonctionnelles qui justifiaient la reconnaissance des processus traditionnels.

## 2. Du principe de neutralité technologique ou de la nécessité d'un cadre juridique équivalent

18. Le principe de neutralité technologique a, à tout le moins, deux significations : la première adresse un conseil de prudence au législateur. Il s'agit lorsqu'il légifère de s'abstenir de toute référence à une technologie particulière qui pourrait interdire par la suite des progrès technologiques (58)... Ainsi, les premières lois sur les signa-

(57) M. DEMOULIN et E. MONTERO, «Le formalisme contractuel à l'heure du commerce électronique», in *Commerce électronique : de la théorie à la pratique*, Cahier du CRID, n° 23, Bruxelles, Bruylant, 2003, p. 161. Voir également D. GOBERT et E. MONTERO, «Le traitement des obstacles formels aux contrats en ligne», in E. MONTERO (Ed.), *Le commerce électronique en fin sur les rails? Analyse et propositions de mise en œuvre de la directive sur le commerce électronique*, Cahier du CRID, n° 19, Bruxelles, Bruylant, 2001, p. 199.

(58) A noter sur l'application de ce principe dans le cadre de la directive 2002/58/CE sur le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, les réflexions de J. DHOST et K. ROSIER, «Directive vie privée et communications électroniques : premiers commentaires», *L'ubiquité*, 2003, n° 15, p. 45. «Par rapport à la directive 97/66/CE, la nouvelle directive est novatrice en ce sens qu'elle prévoit des règles indépendantes de la technologie mise en œuvre. Ce cadre neutre devrait être garant de la certitude juridique et rendre superflue toute modification de la législation en fonction des avancées technologiques...L'effet paradoxal qui en découle est que pour pallier les incertitudes liées à l'évolution technologique future, on recourt à des termes imprécis, qui sont eux-mêmes source d'incertitude juridique.»

tures électroniques, celle de l'Utah, Etat américain, ou de l'Allemagne se sont révélées vite désuètes dans la mesure où la terminologie employée interdisait la reconnaissance de certains procédés de signatures bien plus fiables que ceux que la loi consacrait (59). La seconde signification nous importe plus ici : il s'agit de ne pas réserver un sort différent aux opérations menées via des processus électroniques par rapport à celui consacré pour les opérations conduites par des procédés traditionnels.

19. La loi sur la criminalité informatique du 28 novembre 2000 (60) est fondée sur le principe simple et sain suivant lequel toute opération réprimée off line doit l'être ni plus ni moins lorsqu'elle est réalisée on line (61). Sans doute, vu le principe de l'interprétation stricte des textes pénaux, de nouvelles infractions doivent être créées mais les conditions mises à la reconnaissance de ces infractions doivent-elles être calquées dans toute la mesure du possible sur celles existantes dans le cadre des infractions traditionnelles. La commission d'infractions par l'utilisation de l'électronique ou relatives à des systèmes d'information, d'une part, peut certes rester impunie mais, d'autre part, ne mérite pas non plus un régime visant à tromper une personne physique. L'utilisation de procédés visant à tromper une machine mérite une sanction égale, ni plus ni moins. Sans doute, ce principe dit de neutralité technologique n'a point toujours été respecté lorsqu'on analyse soigneusement les textes et certains déplorent un durcissement de la répression à l'endroit de cette nouvelle forme de criminalité (62) mais tel n'est pas l'objet de notre propos d'aujourd'hui.

(59) Le lecteur voudra bien se référer sur ce point à la démonstration de M<sup>mes</sup> GOBERT et MONTERO, art. cité, p. 73-78 et spécialement le n° 4.

(60) Loi du 28 novembre 2000 relative à la criminalité informatique, *M.B.*, 3 février 2001, p. 2909 et s.

(61) Cf. à cet égard, ce passage de l'exposé des motifs : «Si le droit pénal nécessite certaines modifications pour tenir compte des spécificités de la criminalité informatique et ce afin de respecter le principe «*Nullum crimen sine lege*», il ne faudrait pas que ces adaptations du droit pénal aux progrès technologiques aboutissent à sanctionner un type de comportement alors que si ce même comportement avait été commis sans l'aide de l'informatique, il n'aurait peut-être pas donné lieu à une répression pénale.»

(62) A propos de la définition du «faux en informatique» comparée à celle du «faux en écritures», lire O. LEROUX, note sous Civ. Liège, 18 nov. 2002, *Ubiquité*, 2003, p. 96 et s. A propos du «hacking» ou de l'accès non autorisé à des systèmes d'information, les réflexions de S. DYSOLIER et F. de VILLEFAGNE, «La Belgique sort enfin ses armes contre la cybercriminalité», *Auteurs et Médias*, 2001, p. 60 et s.

*B. – Le droit exige que la technique garantisse des opérations conformes au droit voire améliore la situation des personnes protégées par le droit*

*1. Le principe de proportionnalité ou de réciprocité des avantages*

20. Ce principe pourrait s'exprimer comme suit : le législateur entend, chaque fois que cela est possible, mettre à charge de celui qui utilise la technologie aux fins de développer ses activités professionnelles, certaines obligations supplémentaires qui permettent de rétablir l'équilibre traditionnel des parties en présence (63). La justification du principe est simple, si la technologie accroît les capacités de collecte de traitement, de communication des informations relatives à autrui, si la technologie facilite la conclusion de transactions ou d'opérations administratives, il est indispensable que cette même technologie soit configurée et utilisée de manière telle que la personne concernée, l'administré, le consommateur, le fiché, puisse bénéficier dans une mesure «proportionnée» des avantages de la technologie.

21. Les applications législatives belges de ce principe concernent, à l'heure actuelle, les seuls «services marchands» de la société de l'information. L'étranger nous offre cependant l'exemple d'autres applications possibles en particulier en matière d'administration électronique ou de vie privée.

*a) Proportionnalité et services de la société de l'information*

22. A propos des services marchands de la société de l'information, la directive 2000/31 relative à certains aspects juridiques de la société de l'information déjà citée multiplie à cet égard les obligations desdits «prestataires de services de la société de l'information» d'utiliser les ressources de la technologie et ce à diverses fins : avertir l'internaute du caractère publicitaire de ses messages (64), l'informer de manière aisément accessible des codes de conduite auxquels il se soumet, des différentes étapes suivies pour la conclu-

(63) Nous avons développé ce principe dans deux articles : à propos des réglementations sur le contrat électronique, Y. POULLET, «Contrats électroniques et théorie générale des contrats», *Liber Amicorum L. Simont*, Bruxelles, Bruylant, 2002, p. 469 et s.; en matière de protection des données, «Internet et vie privée : entre risques et espoirs», *J.T.*, 17 février 2001, p. 162, n° 26. in *Le droit des nouvelles technologies*, n° spécial.

(64) Ce qui permettra à l'internaute de les filtrer par des moyens technologiques adéquats.

sion du contrat, des techniques mises à disposition pour l'identification et la correction d'éventuelles erreurs. De telles informations doivent être facilement accessibles à tout moment et téléchargeables (65).

Certains auteurs (66) mettent en évidence selon le même principe que l'obligation de description du bien ou du service offert se conçoit de manière plus sévère en matière de transactions conclues via Internet (67), que l'opposabilité des conditions générales suppose selon le critère de la «raisonnable notice», l'utilisation de techniques non seulement d'hyperliens mais, le cas échéant, d'affichage par pop up, de messages clignotants, etc. (68)

23. Quelques dispositions récentes se fondent sur l'exigence de proportionnalité pour obliger celui qui utilise des technologies à mettre à disposition de l'internaute des moyens électroniques pour faire valoir ses intérêts ou ses droits.

Citons ainsi, dans la directive déjà citée sur les services de la société de l'information, la possibilité de s'opposer via des moyens électroniques au spamming (69), l'obligation du fournisseur de mettre à disposition de l'internaute les moyens de correction des erreurs (70) et, plus précisément, en matière de moyens électroniques de paiement et de signature, les outils

(65) ... par des sigles explicites, dotés d'hyperliens ou de pop up.

(66) En particulier, S. CAVANILLAS MUGICA, «Dix thèses sur la protection du «consommateur électronique» d'après la directive sur la vente et les garanties de consommation», *Ubiquité*, n° 7, 2001, p. 99 et s.

(67) «La façon de rédiger un contrat électronique ne doit pas être perçue comme étant identique à celle d'un contrat papier et le juriste ou l'avocat doivent adapter la règle au medium. En particulier, les critères de lisibilité, de compréhension voire de raisonnabilité risquent de ne pas être perçus de la même façon selon qu'on les analyse sur un document écrit ou sur un document électronique.» (V. GAUTRAIS, «Les contrats en ligne dans la théorie générale du contrat : le contexte nord-américain», in *Le commerce électronique - Le temps des certitudes*, Cahier du CRID, n° 17, Bruxelles, Bruylant, 2000, p. 113).

(68) A propos de ces différentes techniques et de l'obligation de les utiliser pour répondre au standard de la «reasonable notice», lire M. CHISSICK et A. KELMAN, *Electronic Commerce Law and Practice*, Sweet and Maxwell, 1999, p. 85 et s.

(69) Cf. l'article 13.2 de la directive 2002/58/CE relative à la protection des données dans le secteur des communications électroniques qui prévoit l'exercice du droit de s'opposer à tout envoi de messages commerciaux non sollicités. A noter en outre, le considérant qui spécifie qu'il serait utile mais certes non obligatoire que dans un tel cas, l'utilisateur d'un service de communication puisse identifier l'émetteur du message et l'objet de celui-ci et puisse le détruire sans avoir à le télécharger. Voir également, l'article 14 §2 de la loi belge transposant cette directive qui prévoit explicitement l'obligation de mettre à disposition «un moyen approprié d'exercer efficacement ce droit par voie électronique».

(70) Cf. l'article 10 de la directive sur certains aspects juridiques de la société de l'information et l'article 8 §1 3° de la loi belge du 11 mars 2003 transposant la directive.

d'une notification électronique de la perte ou du vol (71) de tels moyens.

### b) Autres applications

24. «L'Electronic Freedom of Information Act» (72) américain contient une disposition intéressante au regard du principe que nous évoquons. Il y est affirmé le devoir de l'Administration de mettre à disposition des citoyens intéressés via un média électronique tout document auquel accès a été réclamé au moins trois fois suivant la loi d'accès aux documents administratifs.

Récemment, une autre législation américaine (73) dite «Federal Data Quality Act» a été adoptée qui prévoit que l'accès d'un citoyen à son dossier administratif doit s'opérer électroniquement. Récemment, une commission suédoise (74) a recommandé l'adoption d'une législation qui garantit le droit pour le citoyen de suivre électroniquement l'avancement de son dossier depuis la naissance de celui-ci jusque et y compris son archivage. A une administration plus efficace grâce à la technologie, doit répondre une administration plus transparente et plus accessible pour les citoyens.

En matière de protection des données, on peut de même envisager que certains droits de la personne concernée, ainsi le droit à

(71) A cet égard, l'article 6 de la loi du 17 juillet 2002 (M.B. 17.8.2002, p.35337) qui parmi les obligations de l'émetteur d'un moyen de paiement, prévoit (art.6) la mise à disposition du titulaire de tous les moyens pour effectuer la notification en cas de vol ou de perte de son instrument.

(72) Sur l'«Electronic Freedom of Information Act» de 1996, lire la thèse de C. de TERWANGNE, *Droit à l'information et droit à la transparence : vers une société de la connaissance*. Thèse de doctorat à paraître dans la collection de cahiers du CRID, Bruxelles, Bruylant, 2003. Cf. également, D.W. SCHARTUM, «What should access legislation be like in the future?», *Yuler-2002*, Lee Bygraeve (éd.), p. 55 et s.

(73) Cette loi de 1999 permet à l'Office of Management and Budget d'émettre des «Guidelines» de manière à maximiser l'intégrité, l'accessibilité, l'efficacité, la transmission et l'utilité des données collectées ou utilisées par l'administration et soumet les administrations à des «reviews» internes et externes. Sur cette loi et les Guidelines, H. BURKERT, «Information Quality within the Public Sector», in *Legal Requirements on the Quality of Information*, Research Colloquium, Univ. of St Gallen, 28-30 Aug. 2002, J.N. DRUEY (Ed.), à paraître.

(74) Sur ces recommandations de la Commission ICT suédoise, lire Seipel, *Information System Quality as a Public Concern*, Research Colloquium, Univ. Of St Gallen, 28-29 Aug. 2002, J.N. DRUEY (Ed.), à paraître. BURKERT (l'information du secteur public : le secret, la transparence et le commerce, *Rev. Fr. adm. Publique*, oct-déc. 1994, p. 588 et les références de l'auteur au principe de proportionnalité, développé par l'auteur américain H.H. Perriotti) parle à cet égard à la suite de l'examen de la loi québécoise sur le droit d'accès, du droit du citoyen «à un temps d'ordinateur», signifiant par là que les fichiers d'administration doivent être programmés de manière telle que les citoyens puissent exercer électroniquement leur droit d'accès.

l'information (75), le droit d'accès et de rectification (76), puissent demain se réaliser par des moyens électroniques.

### 2. Le principe de promotion de solutions technologiques conformes ou améliorant la situation des personnes protégées par le droit

25. A cet égard, l'intervention du droit s'opère de diverses manières : il s'agit d'abord de se réserver le droit d'intervenir en cas de développements technologiques présentant des risques majeurs : pour certains intérêts protégés par le droit il s'agit d'affirmer l'obligation de supporter les risques de défaillance des technologies, pour ceux qui les utilisent et ce, indépendamment de toute idée de faute; il s'agit ensuite en imposant une obligation dite de sécurité, d'obliger ceux qui bénéficient des technologies pour leurs opérations de s'assurer qu'elles sont fiables; il s'agit, enfin, de promouvoir des solutions technologiques notamment de règlement des différends afin de faciliter les recours des utilisateurs.

Parcourons rapidement ces diverses méthodes.

26. La première est illustrée par une disposition de la directive du 12 juillet 2002 relative aux traitements de données à caractère personnel et à la protection de la vie privée dans le secteur des communications électroniques. L'article 14 prévoit qu'en cas de non-conformité d'un équipement terminal aux règles de protection des données, la commission peut prendre des initiatives en matière de standardisation de ceux-ci (77). En d'autres termes, la normalisation technique des équipements terminaux constitue une mesure – certes subsidiaire – d'assurer la protection des données à caractère personnel contre les risques de certains traitements abusifs, risques créés par les choix technologiques.

(75) Ainsi, la possibilité par un simple click d'avoir un accès direct au «Privacy Statement» de l'entreprise et aux diverses informations sur l'identité du responsable voire à la déclaration faite par le responsable auprès de l'autorité de contrôle ou au label spécifique donné par l'organe de labellisation (à l'égard de ce dernier point les réflexions de J. REIDENBERG, «Adapting Labels and Filters for Data Protection», *Cybernews*, 1997, III, 6 disponible sur le site de Lex electronica : <http://www.droit.montreal.ca/pub/cybernews/htm>).

(76) Cf. à cet égard, l'article 6 de la loi du 19 juillet 1991 relative aux registres de la population et aux cartes d'identité, modifié par la récente loi du 25 mars 2003 modifiant la loi sur le registre national qui prévoit un droit d'accès électronique du citoyen aux données contenues sur lui dans le registre national ou sur sa carte d'identité électronique.

(77) Sur cette disposition et son interprétation, lire M.V. PEREZ-ASINARI et S. LOUVEAUX, «Proposal for a directive of the European Parliament and of the Council of personal data and the protection of privacy in the electronic communications sector of 12 July 2000 (COM (2000) 385», *ECCLIP*, 2001.

27. La deuxième méthode est illustrée par de nombreuses dispositions. Ainsi, selon l'article 2B de l'Uniform Commercial Code Américain (78), le recours à un agent électronique pour la conclusion de contrats met à charge sans qu'il soit nécessaire de prouver une faute de celui qui y recourt, les risques d'erreurs de programmation à charge de ce dernier.

Le glissement d'une responsabilité fondée sur la faute à une responsabilité quasi automatique fondée sur le risque créé par l'utilisation des technologies est patent dans d'autres dispositions. La solution est classique en matière de paiements électroniques (79) ou de signatures électroniques (80). Le législateur a transcrit les assertions doctrinales et jurisprudentielles classiques suivant lesquelles en cas de perte ou de vol de la carte ou de confidentialité du numéro secret, le porteur de la carte de paiement était responsable des conséquences de ces faits tant qu'il ne les aura pas signalés à l'organisme émetteur. L'obligation de supporter les risques liés à l'utilisation de système d'information est également présente dans la directive sur certains aspects juridiques de la société de l'information lorsqu'il est affirmé que la commande et l'accusé de réception des messages relatifs à une procédure de commande sont réputés reçus dès leur arrivée au serveur de messagerie, même si la personne destinataire du message n'en a pas encore pris connaissance. En effet dès ce moment, ils sont entrés dans la zone de risque à couvrir par le destinataire du message.

28. L'article 16 de la directive européenne 95/47/CE en matière de protection des données impute, troisième méthode, au responsable du traitement des données à caractère personnel, une obligation

(78) R. NIMMER, «Electronic Contracting: Legal Issues», 14 *Journal of Computer and Information Law*, (1996), p. 211 et s. justifie la solution par la théorie de l'«attribution», qui consiste à faire supporter par celui qui crée une fausse apparence, les risques liés aux conséquences de la création de cette fausse apparence. Sur l'article 2B de l'UCC et la conclusion de contrats par un agent électronique, lire nos réflexions in «La conclusion d'un contrat par un agent électronique», in *Commerce électronique - Le temps des certitudes*, op. cit., p. 120 et s.

(79) A ce propos, l'hypothèse formulée par X. THUNIS (*Responsabilité du banquier et automatization des paiements*, Travaux de la faculté de droit de Namur, n° 17, P.U.N., p. 251): «Notre hypothèse est qu'émerge la qualification de «prestataire de services automatisés» dont la responsabilité se fonde sur une théorie du risque qui ne se réfère plus aux articles 1239 et 1937 du Code civil». A propos de la confirmation de cette hypothèse dans la loi récente du 17 juillet 2002 (*M.B.* 17 août 2002, p. 35337), en particulier de l'article 8 de cette loi, l'article de A. SALAÜN, «Une nouvelle pierre à l'édifice de protection des consommateurs: la loi sur les transferts électroniques de fonds», *J.T.* 2003, p. 210.

(80) Cf. sur ce point l'analyse des dispositions en matière de responsabilité dans la directive européenne en matière de signature électronique et dans la loi type de la CNUDCI in Y. POULLET et J.F. LEROUGE, «La responsabilité des acteurs de l'Internet», Rapports de droit belge in *Actes du Congrès de Brisbane*, Juillet 2002, Bruxelles, Bruylant.

de sécurité dont l'étendue est déterminée par les risques d'atteinte à la confidentialité liés aux caractéristiques du système, à la nature des données traitées et aux règles de l'art en matière de sécurité informatique entendue au sens le plus large (81). C'est dire que le droit impose à celui qui traite des données à caractère personnel le choix de solutions technologiques aptes à minimiser voire à réduire à néant les risques d'atteinte à la vie privée (82).

29. Le dernier type d'intervention du législateur vise une série de mesures visant à promouvoir l'utilisation d'outils technologiques visant à assurer directement ou indirectement la conformité au droit des opérations conclues via des systèmes électroniques. Sur ce point, il est difficile d'être exhaustif mais on retiendra la volonté de définir et de recommander, sans nécessairement les imposer, des normes tantôt techniques, tantôt de comportements (83) qui auront – cela va de soi – une influence sur le «design» y compris technique des sites web du commerce électronique. De même, les recommandations de la Commission européenne et le récent livre vert sur les méthodes alternatives de résolution des litiges et l'utilisation de systèmes électroniques à cet égard (84) visent à faciliter les recours des

(81) A propos de cette obligation de sécurité déduite des législations «Privacy», D. de BODT, «De aangestelde van de gegevensscherming inzake de verwerking van persoonsgegevens», *Computer*, 1999, 279-288.

(82) Même réflexion à propos de l'article 8 de la loi récente sur les instruments de transferts électroniques de fonds qui écarte les règles de responsabilité du porteur de la carte si l'instrument a été utilisé «sans présentation physique et sans identification électronique de l'instrument lui-même». Comme le note A. SALAÜN (art. cité, p. 210), «On trouve ici la principale motivation de la dérogation: éviter que les instruments de transfert électronique de fonds ne puissent être utilisés à distance sans aucune sécurité».

(83) A ce propos les travaux du *mem Institute* de l'Université de St Gallen (<http://www.mem.unisg.ch>) qui lors de sa 4<sup>ème</sup> Conférence «on Information Quality and Knowledge» a dédié une part importante de ses travaux sur «Qualität im Internet». A propos de cette tendance à la normalisation des comportements, lire U. GASSER, «Variationen über Informationsqualität», in *Festschrift für J.N. DREYER*, Schulthess, Zürich, 2002, p. 750 et s. En matière de protection des données, les travaux du Comité européen de normalisation décrits sur le site: <http://www.cenorm.be/iss/Projects/DataProtection.htm> et en matière de décrets des sites web aux dispositions légales de diverses natures, les travaux de l'association suisse de normalisation en matière de «Online-services» (SNV Workshop Agreement SNR 1) disponible sur le site: <http://www.snv.ch/>

(84) A noter à cet égard, les recommandations du 30 mars 1998 (98/257/CE) sur les principes applicables aux organes responsables en matière de résolution extra-judiciaire des conflits (*J.O.* 17 avril 1998) et du 4 avril 2001 (2001/310/CE) sur les principes applicables aux organes extra-judiciaires chargés de la résolution à l'amiable des litiges de consommation. Cf. les résolutions du 30 mars 1999 de la Commission à propos des principes applicables aux organes responsables pour la résolution extra-judiciaire des conflits de consommation et du 13 avril 2000 du Conseil sur la création d'un réseau européen pour la résolution extra-judiciaire des conflits de consommation. Le livre vert de la Commission sur les mécanismes alternatifs de résolution des litiges a été publié le 19 avril 2002 et a donné lieu à une résolution du parlement européen, le 12 mars 2003.

internauts lors de difficultés rencontrées en matière d'opérations du commerce électronique. Deux directives, celle dite «commerce électronique» et celle «services financiers à distance» font écho à cet objectif lorsqu'elles réclament la mise sur pied de mécanismes «adéquats et effectifs» de plaintes et de recours (85).

### CONCLUSIONS

30. Les considérations proposées ci-dessus amènent naturellement l'auteur à quelques recommandations à l'adresse du juriste placé face au défi technologique. La première l'invite à oser pénétrer les arcanes de la technologie non pour s'y noyer mais pour saisir les possibilités énormes de son développement. La technologie n'est pas un donné qui s'impose au juriste mais au contraire est un outil flexible, objet d'options de développement et donc de choix. Sans doute dans les choix pratiqués, certains se révèlent déjà irréversibles mais n'est-ce point la faute des juristes de ne pas avoir, par leur présence dans des cénacles certes difficiles à pénétrer, rappelé les exigences du droit ?

Ces exigences, et c'est la deuxième recommandation, méritent sans doute d'être explicitées et ne peuvent l'être que dans la confrontation des juristes et de ceux qui œuvrent au développement technologique. Il ne peut être question d'opposer a priori les valeurs du droit, d'une part et ce développement, d'autre part. Ainsi, on ne peut affirmer a priori que les mesures techniques constituent la mort du droit d'auteur traditionnel et des valeurs que ce droit véhicule. Il importe de comprendre les mécanismes susceptibles d'être mis au point et de s'interroger à propos de chacun sur la signification des équilibres subtils mis en place par nos législations et l'impact légitime ou non de ce mécanisme sur cet équilibre : ainsi, le «fair use», à l'âge des copies faciles, immédiates et non coûteuses ne peut se concevoir avec la même extension aujourd'hui qu'hier.

Ce travail de retour sur soi auquel la technologie invite le droit exige en retour de la technologie le temps de l'attente. Il ne peut être question, troisième recommandation, de réglementer à la hâte et, soit pour le droit de détruire la possibilité de développements

technologiques, soit pour la technologie de se faire du droit un allié inconscient. Il ne peut être question non plus de ne pas réglementer lorsque l'évaluation démontre la non-conformité du développement ou de certains développements par rapport à des valeurs jugées essentielles dans des sociétés qui doivent rester maîtres de l'outil technologique.

Une quatrième recommandation consiste à concevoir de manière positive le développement de la technologie et d'y trouver la possibilité de réalisation plus efficace de certains droits traditionnels voire l'affirmation de nouveaux droits aptes à corriger les déséquilibres nouveaux qu'introduisent les supports technologiques au profit de certains.

Enfin, dernière recommandation, ce travail le juriste ne peut plus l'entreprendre au seul niveau de l'Etat national. La dimension globale du marché qu'impose la technologie, implique des lieux nouveaux de dialogue voire la recherche de consensus réglementaires. Le droit de l'internet ne peut représenter un plus petit commun dénominateur mais doit permettre à nos diverses sociétés de faire valoir leurs propres valeurs au sein d'enceintes internationales légitimes.

(85) Cf. l'article 17 de la directive déjà citée sur certains aspects juridiques des services de la société de l'information et l'article de la directive du 23 septembre 2002 sur la commercialisation à distance des services financiers également déjà citée.